LETTER TO THE EDITOR

Secure communication with single-photon two-qubit states

Almut Beige[1], **Berthold-Georg Englert**[1,2], **Christian Kurtsiefer**[3]
and Harald Weinfurter[1,3]

[1] Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Strasse 1, 85748 Garching, Germany
[2] Atominstitut, Technische Universität Wien, Stadionallee 2, 1020 Wien, Austria
[3] Sektion Physik, Universität München, Schellingstrasse 4, 80799 München, Germany

E-mail: a.beige@mpq.mpg.de

Abstract
We propose a cryptographic scheme that is deterministic: Alice sends single
photons to Bob, and each and every photon detected supplies one key bit—no
photon is wasted. This is in marked contrast to other schemes in which a
random process decides whether the next photon sent will contribute to the
key or not. The determinism is achieved by preparing the photons in two-
qubit states, rather than the one-qubit states used in conventional schemes. In
particular, we consider the realistic situation in which one qubit is the photon
polarization and the other a spatial alternative. Further, we show how one can
exploit the deterministic nature for direct secure communication, that is *without*
the need for establishing a shared key first.

PACS numbers: 03.67.Dd, 42.79.Sz

1. Introduction

Cryptographic schemes based on the exchange of single photons, each carrying one bit of
information, have been widely discussed in the literature [1]. In some of the schemes, *Alice*
and *Bob* share entangled photon pairs [2]. In others, Bob performs measurements on photons
that Alice sends him [3]. They always need to communicate via a classical channel as well.
Experiments have shown that secure key distribution is possible indeed, even over a distance
of several kilometres [4–6].

The standard procedures, such as the so-called BB84 protocol of [3], are *not* deterministic
in the sense that Bob may or may not get a key bit for the next photon that Alice will send; on
average one key bit is obtained for every two photons transmitted[4]. By contrast, the scheme
we propose here *is* deterministic: Bob gets a key bit for each and every photon sent by Alice.

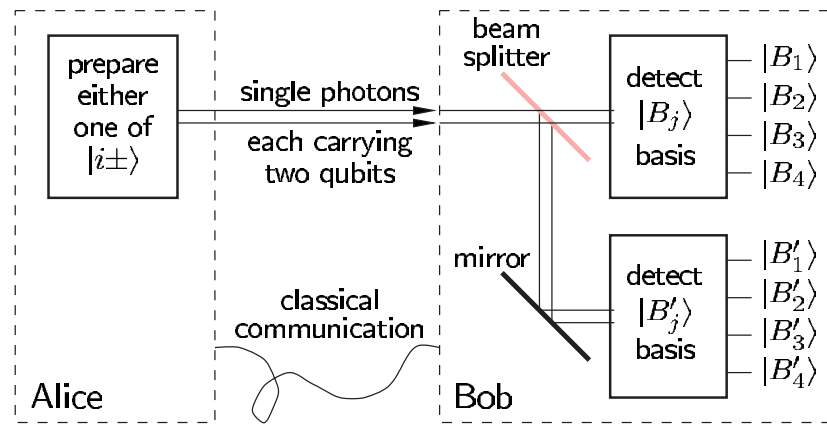[4] Only a few protocols try to go beyond this 50% efficiency [7].

Figure 1. Schematic view of the set-up. To transmit the bit '+' or '−' Alice prepares a photon in one of the states $|i\pm\rangle$ and sends it to Bob. For the purpose of cryptography, two pairs of states are sufficient (e.g., those of (5)), whereas communication requires four pairs (those of (9)). A beam splitter reroutes the photon randomly, and then Bob measures in which state $|B_j\rangle$ or $|B_j'\rangle$ it is. In some cases, communication via the classical channel is required to decode the bit.

   This determinism is the main advantage of our new scheme. It offers, in particular, the option of secure communication without first establishing a shared key.

   To achieve the determinism, Alice sends Bob photons prepared in certain two-qubit states, rather than photons carrying one-qubit states. She uses, for example, the spatial binary alternative of the photon with the basis states $|R\rangle$ and $|L\rangle$ and the two polarization states $|v\rangle$ and $|h\rangle$. Here, $|R\rangle$ and $|L\rangle$ describe a photon travelling in the 'right' or the 'left' fibre, respectively, and $|v\rangle$ and $|h\rangle$ refer to photons with vertical and horizontal polarization.

   With the aid of unitary two-qubit gates [8], Alice can turn any one of the simple product states $|Rv\rangle = |R\rangle \otimes |v\rangle$, $|Rh\rangle$, $|Lv\rangle$ and $|Lh\rangle$ into any desired superposition thereof, so that she can send each photon in the single-photon two-qubit state of her choice. Likewise, Bob's measurements of certain sets of four mutually orthogonal two-qubit states are achieved by appropriate unitary gates. They transform the states of the measurement basis in question into the four basic product states, which are then easily discriminated.

   Since each photon carries two qubits now, the new scheme is not more efficient in terms of qubits than the standard schemes: each qubit pair sent gives one key bit.

2. Quantum key distribution

We present the scheme for key distribution first. It has, of course, a number of features in common with the BB84 protocol, but generates a key bit for every transmitted photon. We discuss its security against eavesdropping and observe that, despite the deterministic nature, it cannot be used for *direct* communication, that is for sending a message without establishing a shared key first. We then introduce a second scheme, with more involved state preparation and analysis, that does enable Alice and Bob to communicate directly and confidentially.

   The experimental set-up of the cryptographic scheme we propose is sketched in figure 1. To transmit one bit, '+' or '−', Alice sends Bob a photon prepared in one of the four states $|i\pm\rangle$ ($i = 1, 2$). For a '+' bit she chooses randomly between $|1+\rangle$ and $|2+\rangle$; for a '−' bit between $|1-\rangle$ and $|2-\rangle$. When the photon arrives at Bob's end, he randomly chooses between two different two-qubit bases for his analysis of the photon state. Experimentally, this can be

Table 1. For the states of (1): key bits as inferred by Bob upon learning which type of photon was sent by Alice. Note that Bob does not need this classical information if he detects the states of the first and fourth columns.

Photon sent by Alice	State detected by Bob			
	B_1 or B_1'	B_2 or B_2'	B_3 or B_3'	B_4 or B_4'
Type 1	+	+	−	−
Type 2	+	−	+	−

achieved by sending the incoming photon through a beam splitter and rerouting it to different measurement devices as shown in figure 1. Bob measures either the basis states $|B_1\rangle, \ldots, |B_4\rangle$ or $|B_1'\rangle, \ldots, |B_4'\rangle$, and he can *always* infer the bit Alice sent. Depending on the outcome of his measurement, he might be able to deduce the incoming bit immediately. In some cases, classical communication is required, and Alice has to tell Bob whether the photon state she prepared was of type '1' or '2'.

For illustration, let us consider the simplest version in which the states sent by Alice and the states detected by Bob are all product states[5] such as

$$(|1+\rangle, |1-\rangle; |2+\rangle, |2-\rangle) = (|Rs\rangle, |La\rangle; |Sv\rangle, |Ah\rangle)$$

$$(|B_1\rangle, |B_2\rangle, |B_3\rangle, |B_4\rangle) = (|Rv\rangle, |Rh\rangle, |Lv\rangle, |Lh\rangle) \tag{1}$$

$$(|B_1'\rangle, |B_2'\rangle, |B_3'\rangle, |B_4'\rangle) = (|Ss\rangle, |As\rangle, |Sa\rangle, |Aa\rangle)$$

where

$$\left.\begin{array}{c}|S\rangle \\ |A\rangle\end{array}\right\} = \frac{1}{\sqrt{2}}(|R\rangle \pm |L\rangle) \qquad \left.\begin{array}{c}|s\rangle \\ |a\rangle\end{array}\right\} = \frac{1}{\sqrt{2}}(|v\rangle \pm |h\rangle) \tag{2}$$

are symmetric (S and s) and antisymmetric (A and a) superpositions of the basic alternatives. Note that each of Bob's states is orthogonal to either the '+' state or the '−' state of each pair; this is the essential property for the deterministic transmission. Suppose, for instance, that Bob detects state $|B_3\rangle = |Lv\rangle$, it is orthogonal to $|1+\rangle = |Rs\rangle$ and $|2-\rangle = |Ah\rangle$ and therefore it signifies '−' if a photon of type '1' was sent and '+' if it was of type '2'. These matters are summarized in table 1.

Let us now exhibit the basic general features of our deterministic scheme, as they are illustrated by this particular example. How can Bob always know which bit Alice sent? He can distinguish the '+' states from the '−' states unambiguously if, for all state pairs $|i+\rangle/|i-\rangle$, each possible measurement result can only be caused by $|i+\rangle$ or $|i-\rangle$, but not by both. This must be the case for every basis measured by Bob. Then he can infer the bit transmitted as soon as Alice identifies the type of pair used (that is she tells him the value of the pair label i).

For the security of the scheme, it is important that the state pairs $|1\pm\rangle$ and $|2\pm\rangle$ sent by Alice are neither identical nor orthogonal. It is equally important that Bob has more than one basis at his disposal, because this is what renders possible the detection of an eavesdropper. In example (1), the two bases are in fact even complementary since the transition probabilities $|\langle B_i|B_j'\rangle|^2 = \frac{1}{4}$ do not depend on the quantum numbers i, j. This maximal incompatibility is not really needed, but the bases should not be very similar to each other in order to ensure that an eavesdropper will surely cause a substantial number of false detections at Bob's end, as we discuss below.

---

[5] Therefore, this particular example could also be realized by exploiting the polarization qubits of paired photons.

To analyse this in more detail, we consider a scheme that is somewhat more general than the one based on the product states (1). Here Bob's bases are related to each other by

$$(|B_1'\rangle, |B_2'\rangle, |B_3'\rangle, |B_4'\rangle) = (|B_1\rangle, |B_2\rangle, |B_3\rangle, |B_4\rangle)\mathbf{K} \tag{3}$$

where the 4×4 matrix $\mathbf{K}$ is given by

$$\mathbf{K} = \frac{1}{1 + k^2}\begin{pmatrix} 1 & k & k & k^2 \\ k & k^2 & -1 & -k \\ k & -1 & k^2 & -k \\ k^2 & -k & -k & 1 \end{pmatrix} \tag{4}$$

with a real parameter k. For brevity and simplicity, we are satisfied with the discussion of the most elementary version of the scheme, where Alice makes use of two state pairs only that are given by

$$\begin{aligned} |1+\rangle &= (|B_1\rangle + k|B_2\rangle)/\sqrt{1 + k^2} \\ |1-\rangle &= (k|B_3\rangle - |B_4\rangle)/\sqrt{1 + k^2} \\ |2+\rangle &= (|B_1\rangle + k|B_3\rangle)/\sqrt{1 + k^2} \\ |2-\rangle &= (k|B_2\rangle - |B_4\rangle)/\sqrt{1 + k^2}. \end{aligned} \tag{5}$$

More generally, she could always use four pairs, and even six pairs in some versions [9]. Relations (5) remain valid if the $|B_j\rangle$ are replaced by the $|B_j'\rangle$. Note that the inverse of the transformation (3) is also furnished by $\mathbf{K}$ since this matrix is both Hermitian and unitary. For $k = 1$, in particular, we return to the situation of (1) where the two bases $|B_j\rangle$ and $|B_j'\rangle$ are complementary. Table 1 continues to apply, irrespective of the value of k.

Let us now imagine that *Evan*, the eavesdropper, is listening in. He intercepts each photon sent by Alice, performs a measurement on it, and then forwards a replacement photon to Bob. Evan will not be able to infer with certainty which two-qubit state is carried by the intercepted photon, and so he has to make an educated guess based on his measurement result. Then he prepares the replacement photon accordingly, namely in the two-qubit state that has the best chance of avoiding wrong detector clicks at Bob's end. If, for instance, Alice has sent a $|1+\rangle$ photon, then the detectors for $|B_3\rangle$ and $|B_4\rangle$ as well as $|B_3'\rangle$ and $|B_4'\rangle$ would yield wrong clicks and reveal the interference of the eavesdropper. Thus, Evan has to solve a two-fold problem: which basis should he measure, and which states should be forwarded to Bob, such that the probability of a wrong click is minimal?

These questions can be answered systematically [9], also for more general intercept–resend strategies, much like the corresponding studies [10] for the BB84 protocol. (The generalizations do not offer a real advantage to Evan, however.) In an optimal strategy then, the probability that Bob will detect a wrong click is

$$p_{\text{min}}^{(2)} = \frac{1}{2} - \frac{1}{2}\frac{\sqrt{1 + k^4}}{1 + k^2}. \tag{6}$$

All other intercept–resend strategies that Evan might employ result in larger error rates. The largest value is obtained for $k = \pm 1$, namely $p_{\text{min}}^{(2)} = (2 - \sqrt{2})/4 = 14.6\%$; for $k = 0$ and $k \to \pm\infty$ the minimal error rate vanishes. Both the limiting cases are easily understood: for $k = \pm 1$ Bob's measurement bases are complementary and therefore maximally incompatible, and for $k = 0$ or $k \to \pm\infty$ they are essentially identical. We note in passing that if four pairs of states are used rather than just the two pairs of (5), the minimal error rate increases to

$$p_{\text{min}}^{(4)} = \frac{1}{2}\frac{\min\{1, k^2\}}{1 + k^2} \tag{7}$$

which can be as large as 25%, and an eavesdropper's presence can then be noticed more easily.

For the purpose of this letter, we continue to focus on the two-pair scheme and assume that Alice and Bob have wisely chosen a k value near $k = 1$. Suppose that they want to establish a key of 1000 bits, and Alice sends 1100 photons in two-qubit states, randomly chosen from the four states of (5). Bob detects all the photons, then selects a random subset of 100 and tells Alice which states he found them in. If some of Bob's measurement results are inconsistent with the states Alice sent, such as detecting $|B_3'\rangle$ for a $|1+\rangle$ photon, then Alice does not trust the transmission and they start all over again. If, however, Bob's results are all right, then Alice concludes that the likelihood that Evan has listened in is less than $\left(1 - p_{\text{min}}^{(2)}\right)^{100} = 1.3 \times 10^{-7}$, which she and Bob have earlier decided to be sufficiently small for the security level they would like to have. Alice then reveals the type of each photon, '1' or '2', and Bob infers the bits sent with the aid of table 1. Thereafter they share a secure 1000-bit key string. A confidential message of this length can then be exchanged.

3. Secure communication without first establishing a shared key

Given the deterministic nature of the scheme, one might wonder if Alice could not send a message directly to Bob without first establishing a shared cryptographic key. It would require that Evan cannot infer the transmitted bits before Alice and Bob become aware of his presence. Now, table 1 shows that Evan could acquire correct knowledge of every second bit sent just by performing the same measurements as Bob does because knowledge of the photon type is not needed in the first and fourth columns. In fact, Evan can improve his educated guesses by choosing his measurement more cleverly [9], since the '+' states sent by Alice are distributed differently over the two-qubit Hilbert space from the '−' states. For example (5), he can systematically exploit the difference between the two-dimensional subspaces spanned by the '+' states and the '−' states to achieve odds as large as $\frac{1}{2} + \frac{1}{2}/\sqrt{1 + k^2}$ for guessing the bits right, which exceeds 85% for $k = 1$. Clearly, secure direct communication is not possible under these circumstances.

But there is a modified scheme that does enable Alice and Bob to communicate directly and confidentially. Again we focus on the simplest version in which Bob's measurement bases are related to each other by

$$
\begin{pmatrix} \langle B_1 | \\ \langle B_2 | \\ \langle B_3 | \\ \langle B_4 | \end{pmatrix} = \frac{i}{\sqrt{3}} \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & -1 & 1 \\ -1 & 1 & 0 & -1 \\ -1 & -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} \langle B_1' | \\ \langle B_2' | \\ \langle B_3' | \\ \langle B_4' | \end{pmatrix}. \tag{8}
$$

Just like $\mathbf{K}$ of (4), the 4×4 transformation matrix appearing here is Hermitian and unitary, so that it also furnishes the inverse transformation. The states sent by Alice are now identical with Bob's basis states, grouped into four pairs of orthogonal states in accordance with

$$
|i+\rangle = |B_i\rangle \qquad |i-\rangle = |B_i'\rangle \qquad \text{for} \quad i = 1, 2, 3, 4. \tag{9}
$$

The basic features discussed above in the paragraphs between (2) and (3) are present here as well.

How Bob infers the bits sent is summarized in table 2. Consider, for example, that he found a certain photon in state $|B_3\rangle$. He will infer that '+' was sent if Alice tells him that it was a type-3 photon because $|B_3\rangle$ is orthogonal to $|3-\rangle$, and that '−' was sent if it was of type 1, 2, or 4 because $|B_3\rangle$ is orthogonal to $|1+\rangle$, $|2+\rangle$ and $|4+\rangle$.

Now, the minimal error rate resulting from eavesdropping of the intercept–resend kind is $\frac{1}{6} = 16.7\%$ for (9) with (8), which is less than 25% of the four-pair key-sharing scheme to

Table 2. For the states of (8) and (9): key bits as inferred by Bob upon learning which type of photon was sent by Alice.

Photon sent by Alice	State detected by Bob							
	B_1	B_2	B_3	B_4	B'_1	B'_2	B'_3	B'_4
Type 1	+	−	−	−	−	+	+	+
Type 2	−	+	−	−	+	−	+	+
Type 3	−	−	+	−	+	+	−	+
Type 4	−	−	−	+	+	+	+	−

Table 3. Direct confidential communication. Alice chooses a random key sequence of 1, 2, 3, 4 (first row) and matches it with the bit sequence of the message (second row) interspersed with randomly located control bits (boxed) to determine the sequence of states to be sent (third row). Bob obtains a sequence of detected states (fourth row). The control bits are used to check for the presence of an eavesdropper. After Alice reveals the random sequence of the first row, Bob can then reconstruct the message of the second row.

Alice's key	1	3	4	4	1	2	1	3	3 ⋯
Message	+	⊞	−	−	−	+	⊟	+	− ⋯
States sent	1+	3+	4−	4−	1−	2+	1−	3+	3 − ⋯
Bob finds	B_1	B'_1	B'_4	B_2	B_2	B'_4	B_4	B_3	B'_3 ⋯

which (7) refers, but more than 14.6% of the two-pair version[6]. Thus, Evan's interference can be detected just as easily in the present scheme of (9) and (8) as in the previous one of (5) and (3) or of (1). Therefore, the scheme defined by (8) and (9) could be used for secure key distribution.

But this scheme is also well suited for direct communication, since the four '+' states span the whole two-qubit Hilbert space uniformly, and the four '−' states do so as well. Thus, Evan cannot distinguish '+' photons from '−' photons here without knowing the photon type. In particular, although the columns of table 2 have 3:1 ratio of the signs, both the kinds carry equal weight. If, for example, $|B_3\rangle$ is detected then $|3+\rangle$ is as likely as $|1-\rangle$, $|2-\rangle$ and $|4-\rangle$ together.

Direct confidential communication is achieved as follows; see table 3. *Step one*: Alice generates, at her end, a random sequence of 1, 2, 3, 4 that will serve as the cryptographic key. Only Alice knows this key. *Step two*: she matches this sequence with the string of +/− message bits, interspersed with a fair number of control bits at random positions, and so determines the two-qubit states to be sent to Bob. Only Alice knows which bits are control bits and which are message bits. *Step three*: Alice sends the photons in these states, and Bob detects them in one of the states of his measurement bases. *Step four*: Alice tells Bob which photons carried control bits, and he tells her in which state he found them. *Step five*: Alice verifies that Bob's findings are consistent with what she sent. If no inconsistencies—that is errors—are noted, Alice concludes that the transmission was secure and continues with step six; otherwise she repeats the procedure beginning with step one. *Step six*: Alice reveals the key sequence of step one, and Bob reconstructs the message with the aid of table 2.

This scheme for direct communication is secure because Alice does not reveal her key sequence until she has convinced herself that Evan has not been listening in. Without this classical information, Evan cannot infer a single bit of the message. The only bits he might

[6] These error rates refer to the situation in which Evan wishes to find out the value of each bit transmitted. Instead, he could settle for just a reasonable likelihood for guessing the bit value right and bargain for a reduced error rate in return. A detailed discussion of compromises of this kind will be presented elsewhere.

decode before his presence is detected are the control bits which, however, are not part of the confidential message.

4. Final remarks

Experimental implementations of our schemes for key distribution and direct communication can be realized with the aid of the universal two-qubit gates that were introduced recently [8]. Concerning practical aspects, we remark that we gain a factor of 2 compared to other cryptography schemes even for imperfect transmission and detection. Redundant encoding can overcome the losses in the communication scheme without revealing information to the eavesdropper. We would also like to note that, rather than using two binary alternatives of single photons, one could, of course, equally well exploit the states of any other four-dimensional Hilbert space.

In summary, we propose a new cryptographic scheme. Under ideal conditions, the scheme is deterministic: Alice and Bob get a key bit for each photon sent, whereas other schemes [2, 3] need at least two photons and are not deterministic. A significant percentage of Bob's measurement results will be wrong if an eavesdropper intercepts the transmission, so that his presence can surely be noticed. In addition, we show how the encoding and deterministic decoding of qubits in a four-dimensional Hilbert space allows direct communication, even without first establishing a shared key.

Acknowledgments

References

[1] Lo H-K, Popescu S and Spiller T 1998 *Introduction to Quantum Computation and Information* (Singapore: World Scientific)
   Bouwmeester D, Ekert A and Zeilinger A 2000 *The Physics of Quantum Information* (Berlin: Springer) and references therein
   Gisin N, Ribory G G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145 a recent review article
[2] Ekert A 1991 *Phys. Rev. Lett.* **67** 661
   Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[3] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore)* (New York: IEEE) p 175
   Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[4] Hughes R J, Luther G G, Morgan G L, Peterson C G and Simon C 1996 Quantum cryptography over underground optical fibers *Advances in Cryptology—Proc. Crypto '96* (Berlin: Springer)
[5] Ribordy G, Gautier J-D, Gisin N, Guinnard O and Zbinden H 1998 *Electron. Lett.* **34** 2116
[6] For recent experiments see
   Jennewein T, Simon C, Weihs G, Weinfurter H and Zeilinger A 2000 *Phys. Rev. Lett.* **84** 4729
   Naik D S, Peterson C G, White A G, Berglund A J and Kwiat P G 2000 *Phys. Rev. Lett.* **84** 4733
   Tittel W, Brendel J, Zbinden H and Gisin N 2000 *Phys. Rev. Lett.* **84** 4737
[7] Goldenberg L and Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239
   Lo H-K, Chau H F and Ardehali M 2000 *Preprint* quant-ph/0011056
   Cabello A 2000 *Phys. Rev. Lett.* **85** 5635
[8] Englert B-G, Kurtsiefer C and Weinfurter H 2001 *Phys. Rev.* A **63** 032303 (reference [18] therein is the present article)
[9] Beige A, Englert B-G, Kurtsiefer C and Weinfurter H 2002 Communicating with qubit pairs *Mathematics of Quantum Computation* ed J-L Brylinski and G Chen (Boca Raton, FL: CRC Press)
[10] Fuchs C A, Gisin N, Griffiths R B, Niu C-S and Peres A 1997 *Phys. Rev.* A **56** 1163